

# Contents

<b>Part I: Cryptography—The People</b> .....	1
<b>1 Introductory Synopsis</b> .....	9
1.1 Cryptography and Steganography .....	9
1.2 Semagrams .....	10
1.3 Open Code: Masking .....	13
1.4 Cues .....	17
1.5 Open Code: Veiling by Nulls .....	19
1.6 Open Code: Veiling by Grilles .....	23
1.7 Classification of Cryptographic Methods .....	24
<b>2 Aims and Methods of Cryptography</b> .....	26
2.1 The Nature of Cryptography .....	26
2.2 Encryption .....	32
2.3 Cryptosystems .....	34
2.4 Polyphony .....	36
2.5 Character Sets .....	39
2.6 Keys .....	41
<b>3 Encryption Steps: Simple Substitution</b> .....	44
3.1 Case $V^{(1)} \dashrightarrow W$ (Unipartite Simple Substitutions) .....	44
3.2 Special Case $V \longleftrightarrow V$ (Permutations) .....	46
3.3 Case $V^{(1)} \dashrightarrow W^m$ (Multipartite Simple Substitutions) .....	53
3.4 The General Case $V^{(1)} \dashrightarrow W^{(m)}$ , Straddling .....	55
<b>4 Encryption Steps: Polygraphic Substitution and Coding</b> .	58
4.1 Case $V^2 \dashrightarrow W^{(m)}$ (Digraphic Substitutions) .....	58
4.2 Special Cases of Playfair and Delastelle: Tomographic Methods....	64
4.3 Case $V^3 \dashrightarrow W^{(m)}$ (Trigraphic Substitutions) .....	68
4.4 The General Case $V^{(n)} \dashrightarrow W^{(m)}$ : Codes .....	68
<b>5 Encryption Steps: Linear Substitution</b> .....	80
5.1 Self-reciprocal Linear Substitutions .....	82
5.2 Homogeneous Linear Substitutions .....	82
5.3 Binary Linear Substitutions .....	86
5.4 General Linear Substitutions .....	86
5.5 Decomposed Linear Substitutions .....	87

5.6	Decimated Alphabets .....	90
5.7	Linear Substitutions with Decimal and Binary Numbers .....	91
<b>6</b>	<b>Encryption Steps: Transposition</b> .....	<b>93</b>
6.1	Simplest Methods .....	93
6.2	Columnar Transpositions .....	98
6.3	Anagrams .....	102
<b>7</b>	<b>Polyalphabetic Encryption: Families of Alphabets</b> .....	<b>106</b>
7.1	Iterated Substitutions .....	106
7.2	Cyclically Shifted and Rotated Alphabets .....	107
7.3	Rotor Crypto Machines .....	110
7.4	Shifted Standard Alphabets: Vigenère and Beaufort .....	127
7.5	Unrelated Alphabets .....	131
<b>8</b>	<b>Polyalphabetic Encryption: Keys</b> .....	<b>139</b>
8.1	Early Methods with Periodic Keys .....	139
8.2	‘Double Key’ .....	141
8.3	Vernam Encryption .....	142
8.4	Quasi-nonperiodic Keys .....	144
8.5	Machines that Generate Their Own Key Sequences .....	145
8.6	Off-Line Forming of Key Sequences .....	156
8.7	Nonperiodic Keys .....	158
8.8	Individual, One-Time Keys .....	161
8.9	Key Negotiation and Key Management .....	165
<b>9</b>	<b>Composition of Classes of Methods</b> .....	<b>169</b>
9.1	Group Property .....	169
9.2	Superencryption .....	171
9.3	Similarity of Encryption Methods .....	173
9.4	Shannon’s ‘Pastry Dough Mixing’ .....	174
9.5	Confusion and Diffusion by Arithmetical Operations .....	180
9.6	DES and IDEA <sup>®</sup> .....	184
<b>10</b>	<b>Open Encryption Key Systems</b> .....	<b>193</b>
10.1	Symmetric and Asymmetric Encryption Methods .....	194
10.2	One-Way Functions .....	196
10.3	RSA Method .....	203
10.4	Cryptanalytic Attack upon RSA .....	205
10.5	Secrecy Versus Authentication .....	208
10.6	Security of Public Key Systems .....	210
<b>11</b>	<b>Encryption Security</b> .....	<b>211</b>
11.1	Cryptographic Faults .....	211
11.2	Maxims of Cryptology .....	220
11.3	Shannon’s Yardsticks .....	225
11.4	Cryptology and Human Rights .....	226

<b>Part II: Cryptanalysis—The Machinery</b>	233
<b>12 Exhausting Combinatorial Complexity</b>	237
12.1 Monoalphabetic Simple Encryptions	238
12.2 Monoalphabetic Polygraphic Encryptions	239
12.3 Polyalphabetic Encryptions	241
12.4 General Remarks on Combinatorial Complexity	244
12.5 Cryptanalysis by Exhaustion	244
12.6 Unicity Distance	246
12.7 Practical Execution of Exhaustion	248
12.8 Mechanizing the Exhaustion	251
<b>13 Anatomy of Language: Patterns</b>	252
13.1 Invariance of Repetition Patterns	252
13.2 Exclusion of Encryption Methods	254
13.3 Pattern Finding	255
13.4 Finding of Polygraphic Patterns	259
13.5 The Method of the Probable Word	259
13.6 Automatic Exhaustion of the Instantiations of a Pattern	264
13.7 Pangrams	266
<b>14 Polyalphabetic Case: Probable Words</b>	268
14.1 Non-Coincidence Exhaustion of Probable Word Position	268
14.2 Binary Non-Coincidence Exhaustion	271
14.3 The De Viaris Attack	272
14.4 Zig-Zag Exhaustion of Probable Word Position	280
14.5 The Method of Isomorphs	281
14.6 A clever brute force method: EINSing	287
14.7 Covert Plaintext-Cryptotext Compromise	288
<b>15 Anatomy of Language: Frequencies</b>	290
15.1 Exclusion of Encryption Methods	290
15.2 Invariance of Partitions	291
15.3 Intuitive Method: Frequency Profile	293
15.4 Frequency Ordering	294
15.5 Cliques and Matching of Partitions	297
15.6 Optimal Matching	303
15.7 Frequency of Multigrams	305
15.8 The Combined Method of Frequency Matching	310
15.9 Frequency Matching for Polygraphic Substitutions	316
15.10 Free-Style Methods	317
15.11 Unicity Distance Revisited	318
<b>16 Kappa and Chi</b>	320
16.1 Definition and Invariance of Kappa	320
16.2 Definition and Invariance of Chi	323
16.3 The Kappa-Chi Theorem	325
16.4 The Kappa-Phi Theorem	326
16.5 Symmetric Functions of Character Frequencies	328

<b>17</b>	<b>Periodicity Examination</b>	330
17.1	The Kappa Test of Friedman	331
17.2	Kappa Test for Multigrams	332
17.3	Cryptanalysis by Machines: Searching for a period	333
17.4	Kasiski Examination	339
17.5	Building a Depth and Phi Test of Kullback	345
17.6	Estimating the Period Length	348
<b>18</b>	<b>Alignment of Accompanying Alphabets</b>	350
18.1	Matching the Profile	350
18.2	Aligning Against Known Alphabet	354
18.3	Chi Test: Mutual Alignment of Accompanying Alphabets	358
18.4	Reconstruction of the Primary Alphabet	363
18.5	Kerckhoffs' Symmetry of Position	365
18.6	Stripping off Superencryption: Difference Method	370
18.7	Decryption of Code	373
18.8	Reconstruction of the Password	373
<b>19</b>	<b>Compromises</b>	375
19.1	Kerckhoffs' Superimposition	375
19.2	Superimposition for Encryptions with a Key Group	377
19.3	COLOSSUS	401
19.4	Adjustment 'in depth' of Messages	412
19.5	Cryptotext-Cryptotext Compromises	419
19.6	Cryptotext-Cryptotext Compromise: ENIGMA Indicator Doubling	431
19.7	Plaintext-Cryptotext Compromise: Feedback Cycle	448
<b>20</b>	<b>Linear Basis Analysis</b>	459
20.1	Reduction of Linear Polygraphic Substitutions	459
20.2	Reconstruction of the Key	460
20.3	Reconstruction of a Linear Shift Register	461
<b>21</b>	<b>Anagramming</b>	464
21.1	Transposition	464
21.2	Double Columnar Transposition	467
21.3	Multiple Anagramming	467
<b>22</b>	<b>Concluding Remarks</b>	470
22.1	Success in Breaking	471
22.2	Mode of Operation of the Unauthorized Decryptor	476
22.3	Illusory Security	482
22.4	Importance of Cryptology	484
	Appendix: Axiomatic Information Theory	487
	Bibliography	497
	Index	501
	Photo Credits	525

**Decrypted Secrets**

**Methods and Maxims of Cryptology**

Bauer, F.L.

2007, XIV, 525 p. 183 illus., 16 illus. in color., Hardcover

ISBN: 978-3-540-24502-5